U.S. Federal Public Trust TLS PKI Certificate Policy

DRAFT FOR FINAL REVIEW

Version 0.2

February 1, 2018

1. INTRODUCTION

1.1 Overview

This Certificate Policy (CP) outlines the policy and requirements for the United States (U.S.) Federal Public Key Infrastructure in the issuance and management of U.S. Federal Publicly Trusted TLS Certificates. The certificates under this policy are for identifying and authenticating U.S. Federal Government web services.

This policy is for a hierarchical Public Key Infrastructure restricted to services operated by or on behalf of the U.S. Federal Government. The hierarchical PKI is referenced as the **U.S. Federal Public Trust TLS PKI** in this document.

This document serves two purposes:

- To specify the U.S. Federal Public Trust TLS PKI Certificate Policy and requirements, and
- To provide requirements for what each Certification Authority shall address in its Certification Practice Statement

This policy promotes automation to improve U.S. Federal Government efficiencies. This policy also incorporates Certificate Transparency as a key component for publicly accessible and accountable services operated by the U.S. Federal Government.

This policy is applicable to all Certification Authorities within a chain of trust under the **U.S. Federal TLS Root CA**.

The terms and provisions of this certificate policy shall be interpreted under and governed by applicable Federal law.

1.1.1 Scope

The scope of the U.S. Federal Public Trust TLS PKI includes the Certification Authorities used for issuing and managing Transport Layer Security (TLS) certificates for U.S. Federal Government services. The scope is limited to:

- Services that resolve at a registered Internet sub-domain under the .gov and .mil Top Level Domains
- Services that are accessible on the Internet

U.S. Federal Government departments and agencies own and operate services that are not accessible on the Internet and are only accessible from the U.S. Government's intranets and internal networks. These intranet only services should consider using TLS certificates from CAs used for the Federal Enterprise in lieu of the Publicly Trusted certificates covered under this policies. The Federal Enterprise CAs could include only

locally trusted CAs operated by the department or agency or a CA operated under one of the other Federal PKI certificate policies.

The intranet only services may apply for TLS certificates issued under this policy if: i) the identification and authentication requirements (section 3) can be met in entirety, and ii) the information to be contained in the certificate can be publicly disclosed without any redaction.

1.1.2 Compliance

This Certificate Policy conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Baseline Requirements, those Baseline Requirements take precedence over this document.

1.1.3 Certificate Types

This Certificate Policy defines five (5) different types of certificates. Certificates issued under this policy are categorized as CA Certificates or Subscriber Certificates.

1.1.3.1 CA Certificates

A certificate is a CA certificate if the basicConstraints extension is present and has cA:TRUE. CA certificates allowed to be issued under this policy are categorized as Root CA certificates and Subordinate CA certificates.

1.1.3.1.1 Root CA Certificates

A CA certificate is a Root CA certificate if the certificate's issuer and subject are the same and the digital signature may be verified by the public key bound into the certificate.

1.1.3.1.2 Subordinate CA Certificates

A CA certificate is a Subordinate CA certificate if the certificate's issuer and the subject are not the same. Subordinate CA certificates, issued under this policy, have a Path Length Constraint set to zero (0) and Name Constraints specifying permitted dnsName sub-trees only for the .gov and .mil Top Level Domains.

1.1.3.2 Subscriber Certificates

A certificate is a Subscriber certificate if it is not a CA Certificate. Subscriber certificates are end entity certificates as defined in RFC5280 and issued to subjects that are not authorized to issue certificates. Subscriber certificates allowed to be issued under this policy are categorized as Domain Validation TLS Server Authentication certificates, Organization Validation TLS Server Authentication certificates, or Delegated OCSP

Responder signing certificates. CAs shall not issue Subscriber Certificates that simultaneously meet the criteria of more than one of these categories.

1.1.3.2.1 Domain Validation TLS Server Authentication Certificates

A Domain Validation TLS Server Authentication, issued under this policy: i) does not contain any information in the subject distinguished name other than commonName (OID 2.5.4.3) and countryName (OID 2.5.4.6), and ii) asserts a key purpose of id-kp-serverAuth (OID 1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.3.2.2 Organization Validation TLS Server Authentication Certificates

An Organization Validation TLS Server Authentication certificate, issued under this policy: i) contains commonName (OID 2.5.4.3), stateOrProvinceName (OID 2.5.4.8), organizationName (OID 2.5.4.10) and countryName (OID 2.5.4.6) in the subject distinguished name, and ii) asserts a key purpose of id-kp-serverAuth (OID 1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.3.2.3 Delegated OCSP Responder Certificates

A certificate is a Delegated OCSP Responder Certificate if it has a key purpose of id-kp-OCSPSigning (OID 1.3.6.1.5.5.7.3.9) in the Extended Key Usage certificate extension.

1.2 Document name and identification

This is the U.S. Federal Public Trust TLS PKI Certificate Policy.

The following Certificate Policy identifiers are registered by the U.S. Government and reserved for use by CAs as a means of asserting compliance with this CP:

OID	Purpose
{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) arcfbca-policies(3) domain-validated(43) } (2.16.840.1.101.3.2.1.3.43)	Domain Validation TLS Server Authentication Certificates
{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) arcfbca-policies(3) organization-validated(44) } (2.16.840.1.101.3.2.1.3.44)	Organization Validation TLS Server Authentication Certificates

The following Certificate Policy identifiers are registered by the CAB Forum and reserved for use by CAs as a means of asserting compliance with the Baseline Requirements:

OID	Purpose

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1) } (2.23.140.1.2.1)	Domain Validation TLS Server Authentication Certificates
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2) } (2.23.140.1.2.2)	Organization Validation TLS Server Authentication Certificates

Additional documents related to the U.S. Federal Public Trust TLS PKI, including Certification Practice Statement(s), Audit Letter(s), and any applicable Subscriber Agreement(s) can be found at <INSERT URL HERE>.

In accordance with RFC 3647, this CP includes all nine sections of the RFC 3647 framework and an additional addendum with the certificate profiles.

This document was originally based on the CAB Forum Baseline Requirements, which is licensed under the Creative Commons Attribution 4.0 International License. All additions and modifications made to create this CP are in the United States public domain as works of the U.S. Government, and released internationally under the Creative Commons (CCO) 1.0 Universal Public Domain dedication.

1.2.1 Revisions

Ver.	Change Proposal	Description	Adopted	Effective Date
1.0.0	None	Version 1.0 of the Certificate Policy Adopted	<TBD>	<TBD>

1.3 PKI Participants

1.3.1 Federal CIO Council

The U.S. Government's Federal CIO Council was codified by the E-Government Act of 2002. The Federal CIO Council is the principal interagency forum for improving Federal agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources

The Federal CIO Council is comprised of: 1) the Chief Information Officers (CIOs) and Deputy CIOs from 28 U.S. Government Federal executive agencies; 2) liaisons from the

Chief Acquisitions Officers, Chief Financial Officers, and Chief Human Capital Officers; 3) representatives from the Office of Information and Regulatory Affairs; 4) representatives from the Office of Science and Technology Policy; and 5) other groups selected by the CIO Council's Executive Committee.

The Federal CIO Council has established the framework for the Federal PKI (FPKI) and governance of the U.S. Federal Public Trust TLS PKI.

1.3.2 Federal Public Key Infrastructure Policy Authority

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a sub-council comprised of U.S. Federal Government agency representatives and is chartered under the Federal CIO Council.

The FPKIPA is responsible for:

- Maintaining this CP
- Approving the CPS for each CA that issues certificates under this policy
- Reviewing and approving the compliance audits for each CA issuing certificates under this policy
- Ensuring continued conformance of each CA that issues certificates under this policy with applicable requirements as a condition for allowing continued participation
- Ensuring compliance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by CAB Forum
- Ensuring compliance with any additional trust store operator requirements that the U.S. Federal Public Trust TLS Root CA pursues or has inclusion in
- Ensuring compliance with any additional browser requirements that are defined by browser software vendors

1.3.3 Certification Authorities

The U.S. Federal Public Trust TLS PKI CAs are operated on behalf of the U.S. Government. The CAs are responsible for the creation, issuance and management of Certificates including:

- Publication of certificates
- Revocation of certificates
- Operation of certificate status services
- Operating automated services or procedures to perform validation of domain authorization or control as specified in section 3.2.2.4
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP

The CAs operated under this policy provide services to U.S. Government entities which may be part of the Executive Branch, Legislative Branch and Judicial Branch of the Federal Government. The services shall not be provided to the general public, commercial entities, U.S. State, Local, Territorial, Native Sovereign Nations, or international government entities.

1.3.4 Registration Authorities

This policy allows for persons who may not be affiliated with the same U.S. Federal Government organizational unit that is operating the CA to assist in the certificate application process and be designated as an Enterprise Registration Authority.

A CA may designate an Enterprise Registration Authority (RA) to verify certificate requests from the Enterprise RA's affiliated U.S. Federal Government organizational unit. The CA shall not accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA shall confirm that the requested Fully-Qualified Domain Name(s) are within the RA's affiliated U.S. Federal Government organizational unit verified Domain Namespace(s) as registered in the .gov and .mil gTLDs Domain Name Registrars.
2. The CA should confirm that the requested Fully Qualified Domain Name(s) are not within any Domain Namespace(s) for any U.S. State, Local, Territorial, Native Sovereign Nations, or any other entities identified as a *Non-Federal Agency* in the .gov Domain Name Registrar per United States Code (U.S.C.) 41 CFR Part 102-173.

The CA shall impose these limitations through an agreement with the Authorizing Authority of the Domain Namespace as defined under United States Code (U.S.C.) 41 CFR Part 102-173. The CA shall monitor compliance by the RA and institute technical controls. The CA shall use both audits and analytics based methods, such as monitoring of Certificate Transparency Log(s) and other services, to ensure compliance.

Delegated Third Parties are not allowed as Registration Authorities.

1.3.5 Subscribers

A Subscriber is the entity identified in a Certificate, capable of using the Private Key that corresponds to the Public Key listed in the certificate, and has agreed to the Terms of Use with the CA. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

For this policy, Subscribers are limited to:

1. Web services operated by or on behalf of U.S. Government agencies
2. Domain Names within the .gov and .mil Domain Namespace(s)

1.3.6 Relying Parties

A Relying Party is any individual or entity that relies on a U.S. Federal Public Trust TLS PKI Certificate, the information included in the certificate, and the digital signature by a CA.

For this policy, Relying Parties may include individuals or entities accessing U.S. Government web services available on the Internet.

Relying Parties should verify the validity of certificates via revocation services provided for all certificates prior to relying on certificates. Certificate Revocation List (CRL) and On-line Certificate Status Protocol (OCSP) service location information is provided within certificates.

1.3.7 Other Participants

CAs operating under this policy require the services of Qualified Auditors to perform independent, annual assessments on the conformance of the CA's practices and procedures. Qualified Auditor requirements are covered in section 8.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This policy is limited to Publicly Trusted TLS Certificates used for identifying and authenticating U.S. Federal Government web services. Certificates may be used for all legal authentication and encryption purposes.

1.4.2 Prohibited Certificate Uses

Certificates may not be used where prohibited by law.

Certificates for identifying natural persons are not allowed under this policy including but not limited to identity certificates used to identify natural persons for digital signatures, S/MIME, client authentication, and encryption. CAs may not issue Subscriber certificates for natural persons or enter into any cross-certification with any CAs that issue certificates used to identify and authenticate natural persons.

1.5 Policy administration

1.5.1 Organization Administering the Document

The FPKIPA is responsible for administering this document.

1.5.2 Contact Person

Contact information for the FPKIPA is fpki@gsa.gov.

1.5.3 Person Determining CPS suitability for the policy

The FPKIPA shall affirm the suitability of any CPS to this policy.

1.5.4 CPS approval procedures

A CPS shall be submitted and approved by the FPKIPA.

Prior to submitting a CPS, the CA shall perform a compliance analysis culminating in a written report that provides a summary of areas in which the CPS may not or does not comply with this CP. The CA shall resolve these discrepancies prior to submitting the CPS to the FPKIPA. The CA shall have an approved CPS, meet all CP and CPS requirements, conduct Federal Information Security Modernization Act assessment and authorization activities, and produce an authority to operate prior to commencing operations.

CAs shall review their CPS and perform an annual self-assessment for compliance with this CP at least every 365 days. After review and approval, the CPS document version number and a dated changelog entry shall be added, even if no other changes were made to the document.

1.6 Definitions and Acronyms

1.6.1 Definitions

Capitalized terms used in this CP shall have the meanings defined in Appendix A.

1.6.2 Acronyms

See Appendix B for a complete list of acronyms and abbreviations used in this CP.

1.6.3 References

See Appendix C for a complete list of standards and other references included in this CP.

1.6.4 Conventions

The key words “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this CP shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Each CA shall disclose the following information through a publicly accessible Repository:

- CA Certificates
- Certificate Revocation Lists (CRLs) for all issued certificates
- Online Certificate Status Protocol responses for all issued certificates
- CPS documents
- Terms of Use Agreements
- Audit Letters

CPS documents and Audit Letters shall not be redacted.

Each CA shall ensure that its Certificate from the Root CA and the certificate status services for issued certificates are available through a Repository 24 hours a day, 7 days a week with a minimum of 99.5% availability overall per year.

2.2 Publication of information

The FPKIPA shall publicly post this CP on <INSERT URL>, ensuring it is readily accessible on a 24x7 basis.

Each CA shall disclose the following information through a publicly accessible Repository:

- CA Certificates
- Certificate Revocation Lists (CRLs) for all issued certificates
- Online Certificate Status Protocol responses for all issued certificates
- CPS documents
- Terms of Use Agreements
- Audit Letters

CPS documents and Audit Letters shall not be redacted.

CAs shall publish pre-certificates for any Domain Validation TLS Server Authentication Certificates and Organization Validation TLS Server Authentication Certificates to Certificate Transparency Logs.

Web pages that allow for testing certificate validation up to the U.S. Federal Public Trust TLS Root CA can be found at:

- https://valid.tlsroot.pki.gov
- https://revoked.tlsroot.pki.gov
- https://expired.tlsroot.pki.gov

2.3 Time or frequency of publication

The FPKIPA and CAs shall update and publish the CP and CPS documents within thirty (30) days after being approved.

Each CA shall post to the Repository any issued CA Certificate as soon as possible after issuance but no later than fifteen (15) days after issuance. The FPKIPA or designee shall disclose and submit the CA Certificate, CPS, and Audit Letter(s) to trust store operators and applicable databases, such as the Common CA Database, as required by the trust store operator policies.

Each CA shall publish CRLs in accordance with section 4.9.7.

2.4 Access controls on repositories

Each CA shall make its Repository publicly available in a read-only manner. Repository information shall be protected from unauthorized modification.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

This policy restricts the subject names of CAs. CAs that issue certificates under this policy shall have distinguished names using geo-political names consisting of country, organization, and common name. Organization units may only be used with approval by the FPKIPA.

End-entity certificates issued under this policy shall use distinguished names and subject alternative names that comply with section 7 and the certificate profiles in Appendix D.

3.1.2 Need for names to be meaningful

End-entity certificates issued under this policy shall have a common name that is one of the domain names validated in accordance with section 3.2.2.4.

3.1.3 Anonymity or pseudonymity of subscribers

A CA shall not issue anonymous certificates. CA certificates shall not contain anonymous or pseudonymous identities.

Relying parties should consider certificates to be issued by the U.S. Government for U.S. Government assets and all Subscribers to be affiliated with the U.S. Government.

3.1.4 Rules for interpreting various name forms

Distinguished names in certificates are interpreted using the X.500 Standard and the ASN.1 syntax.

3.1.5 Uniqueness of names

The common name attribute for CA Certificates shall be unique from all other CA Certificates.
There is no stipulation for the uniqueness of the Subject information in Subscriber certificates.

3.1.6 Recognition, authentication, and role of trademarks

CAs shall not issue a certificate that knowingly infringes any trademark. The FPKIPA shall resolve disputes involving names and trademarks.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The CA shall verify the Applicant has possession of the Private Key that corresponds to the Public Key in the certificate request.

As one method to verify possession of the Private Key, the CA may verify the digital signature on a certificate signing request that was created using the Private Key. The FPKIPA may allow other methods that are at least as secure as those cited here.

3.2.2 Authentication of Organization and Domain Identity

All Domain Validation TLS Server Authentication certificates issued under this CP shall include Subject Identity Information of commonName. Domain Validation TLS Server Authentication certificates may include Subject Identity Information of countryName. If the Applicant requests a Domain Validation TLS Server Authentication certificate that will contain Subject Identity Information to include countryName field, then the CA shall verify the country associated with the Subject using a verification process meeting the requirements of section 3.2.2.3.

All Organization Validation TLS Server Authentication certificates issued under this CP shall include Subject Identity Information of commonName, countryName, organizationName and stateOrProvinceName and shall not include any other Subject Identity Information. If the Applicant requests a Certificate that will contain Subject Identity Information comprised of the countryName field and organizationName and stateOrProvinceName, then the CA shall verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements in section 3.2.2.1.

3.2.2.1 Identity

This CP is restricted to the generic Top Level Domains (gTLDs) for .gov and .mil which are registered as the sub-category of *sponsored* TLDs (sTLDs) with ICANN.

The .gov sTLD is sponsored by the U.S. Government's General Services Administration. The .gov regulations are defined in 41 CFR Part 102-173. Under 41 CFR Part 102-173.30, registration in the .gov domain is only available to official governmental organizations in the United States including Federal (U.S. Government), State and local governments, and Native Sovereign Nations.

The .mil sTLD is sponsored by the U.S. Government's Department of Defense. The .mil domain exists for the exclusive use of the Department of Defense and is referenced in Department of Defense Instruction (DoDI) 8410.01.

The Domain Name Registrars for both .gov and .mil are managed by the U.S. Government.

All three branches of the U.S. Government have primary headquarters located in the city of Washington in the District of Columbia in the United States of America. Any Organization Validation TLS Server Authentication certificate issued under this CP shall be for U.S. Government mission purposes and for consumers, partners, and other relying parties to identify the U.S. Government as the subject. For Organization Validation TLS Server Authentication certificates, the CA shall verify that the Applicant is under authority of one of the three branches of the U.S. Government and this verification is sufficient to assert the organizationName of the U.S. Government (o=U.S. Government) and assert the stateOrProvinceName as District of Columbia.

Verification may rely upon the .gov and .mil Domain Name Registrars.

3.2.2.2 Doing Business As (DBA) and/or Tradename

Subject Identity Information shall not include a DBA or tradename.

3.2.2.3 Verification of Country

All CAs shall verify the inclusion of subject:countryName in Subscriber certificates by one of the following:

- The requested Domain Name is within the .mil or .gov sTLD domain space
- Information provided by the Domain Name Registrar

3.2.2.4 Validation of Domain Authorization or Control

CAs shall confirm that, as of the date the Certificate was issued, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed in section 3.2.2.4.x.

This CP allows for procedures adhering to the Baseline Requirements and is limited to four (4) validation methods:

- Section 3.2.2.4.5 Domain Authorization Document
- Section 3.2.2.4.6 Agreed-Upon Change to Website
- Section 3.2.2.4.7 DNS Change
- Section 3.2.2.4.10 TLS Using a Random Number

Wildcard FQDNs are not allowed to be validated using section 3.2.2.4.6 Agreed Upon Change to Website or section 3.2.2.4.10 TLS Using a Random Number. All wildcard domain names included in a certificate shall require validation by either section 3.2.2.4.7 DNS Change, or section 3.2.2.4.5 Domain Authorization Document signed by the Domain Contact authorizing the issuing of a certificate to include the wildcard FQDN.

CAs shall maintain a record of which domain validation method, including the relevant Baseline Requirements version number, was used to validate each domain in a certificate.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation shall have been completed within the time period specified in section 4.2.1 of this policy prior to certificate issuance.

For purposes of domain validation, the term Applicant includes the Applicant's U.S. Government Department, Agency, Commission, component, or other organizational unit defined in United States Code.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.3 Phone Contact with Domain Contact

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.4 Constructed Email to Domain Contact

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.5 Domain Authorization Document

This validation method confirms the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document.

The Domain Authorization Document shall substantiate that the communication came from the Domain Contact. The CA shall verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data provided by .mil or .gov has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

3.2.2.4.6 Agreed-Upon Change to Website

This validation method confirms the Applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content shall not appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value shall not appear in the request.

If a Random Value is used, the CA shall provide a Random Value unique to the certificate request and shall not use the Random Value after 30 days.

A Request Token shall incorporate the key used in the certificate request. A Request Token may include a timestamp to indicate when it was created and other information to ensure its uniqueness. A Request Token that includes a timestamp shall remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp shall be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA shall not re-use it for a subsequent validation.

The binding shall use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data.

The CA shall define in its CPS the format of Request Tokens it accepts and shall document the "/.well-known/pki-validation/" directory and any other paths registered with IANA.

3.2.2.4.7 DNS Change

This validation method confirms the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record for either:

1. An Authorization Domain Name
2. An Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after 30 days.

A Request Token shall incorporate the key used in the certificate request. A Request Token may include a timestamp to indicate when it was created and other information to ensure its uniqueness. A Request Token that includes a timestamp shall remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp shall be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA shall not re-use it for a subsequent validation.

Once the FQDN has been validated using this method, the CA may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. For example, a validation for the example "myapp.mydomain.gov" may be used during the timeframe permitted for reuse of validation information to issue a certificate that includes "home.myapp.mydomain.gov".

3.2.2.4.8 IP Address

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.9 Test Certificate

This validation method defined by the Baseline Requirements is not allowed under this CP.

3.2.2.4.10. TLS Using a Random Number

This validation method confirms the Applicant's control over the requested FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

If a Random Value is used, the CA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after 30 days.

3.2.2.5 Authentication for an IP Address

IP Addresses are not allowed in the certificate profiles under this CP.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName, the CA shall establish and follow a documented procedure and technical controls that determines if the wildcard character occurs in the first label position to the left of the .gov and .mil suffixes (e.g. *.gov, *.mil). If a wildcard would fall within the label immediately to the left of the .gov and .mil suffixes (e.g. *.gov, *.mil), the CA shall refuse issuance. All CAs are prohibited from issuing any Wildcard Certificate to the entire sTLDs for .gov and .mil.

Wildcard FQDNs are not allowed to be validated using section 3.2.2.4.6 Agreed Upon Change to Website or section 3.2.2.4.10 TLS Using a Random Number. All wildcard FQDNs included in a certificate shall require validation by section 3.2.2.4.7 DNS Change, or section 3.2.2.4.5 Domain Authorization Document signed by the Domain Contact authorizing the issuing of a certificate to include the wildcard FQDN.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA should consider the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Databases maintained by the CA or affiliated government agencies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under section 3.2 and sub-sections.

3.2.2.8 Certification Authority Authorization (CAA) Records

For Domain Validation TLS Server Authentication certificates and Organization Validation TLS Server Authentication certificates, CAs shall verify CAA records.

When processing CAA records, CAs shall process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags may be supported, but shall not conflict with or supersede the mandatory property tags set out in this policy. CAs shall respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.

CAA checking is optional for certificates only when a Certificate Transparency pre-certificate was created and logged in at least two public logs, and CAA records were checked for the pre-certificate.

CAs are permitted to treat a record lookup failure as permission to issue only if all the following are true:

- The failure is outside the CA's infrastructure
- The lookup has been retried at least once
- The domain's zone does not have a DNSSEC validation chain to the ICANN root

CAs shall document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback on the circumstances, and should dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.3 Authentication of individual identity

Subscriber certificates identifying and authenticating natural born persons or individual identity shall not be issued under this policy.

3.2.4 Non-verified subscriber information

Non-verified subscriber information shall not be asserted in any certificates under this Certificate Policy.

3.2.5 Validation of authority

A CA may use the sources listed in section 3.2.2.1 to verify the Applicant is under authority of the U.S. Government and assert organizationName of U.S. Government.

In addition, a CA may establish a process that allows an Authorizing Authority of a .gov or .mil sub-domain to specify the individuals who may request Certificates. If an Authorizing Authority specifies, in writing, the individuals who may request a Certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Authorizing Authority with a list of its authorized certificate requesters upon the Authorizing Authority's verified written request.

3.2.6 Criteria for Interoperation or Certification

CAs shall not have Cross Certificate(s) that identify the CA as the Subject without explicit written permission of the FPKIPA. Any Cross Certificates shall be disclosed publicly, submitted to one or more Certificate Transparency Logs, published to the Repository, and identified in the update to the CPS.

3.3 Identification and authentication for re-key requests

Re-key requests are not allowed under this policy. All requests are treated as new certificate requests.

3.4 Identification and authentication for revocation request

Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

An application for a CA Certificate shall be submitted by an authorized representative of the applicant CA.

An application for a subscriber certificate shall be submitted to the CA by the Applicant, an Applicant Representative, or an RA on behalf of the Applicant.

In accordance with section 5.5.2, all CAs shall maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. All CA shall use this information to identify subsequent suspicious certificate requests.

4.1.2 Enrollment process and responsibilities

The FPKIPA is responsible for approving or denying requests for CA certificate issuances by any CA.

Prior to the issuance of any Certificate, all CAs shall obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The certificate request shall contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

The CA shall be responsible for validating the information in the certificate request and the identity evidence to ensure the information is:

- Properly formed
- Accurate
- Meets the requirements for the type of certificate requested such as a Domain Validation TLS Server Authentication certificate, an Organization Validation TLS Server Authentication certificate, a OCSP Delegated Responder certificate, or a CA Certificate

All communications supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the requested public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

All CAs shall specify the procedures for validating information and identity evidence in the CA CPS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All CAs shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

For Domain Validation TLS Server Authentication certificates and Organization Validation TLS Server Authentication certificates:

- The Applicant information shall include at least one Fully-Qualified Domain Name.
- All Fully-Qualified Domain Names shall be verified in accordance with section 3.2 before issuance of the certificate.
- CAA records for .gov and .mil domains shall be checked prior to issuance of any certificate and the CA shall act in accordance to the requirements in section 3.2.2.8.

The CA shall identify in section 4.2 of the CPS the Issuer Domain Name to be used for CAA records. For example, the CA CAA domain is ‘pki.gov’.

The CA may reuse the documents and data provided in section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under section 3.2 no more than 395 days prior to issuing the Certificate.

All Subordinate CAs shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests for .gov and .mil assets prior to the Certificate’s approval.

Delegated Third Parties are not allowed under this policy and shall not participate in the performance of identification functions.

4.2.2 Approval or rejection of certificate applications

This CP is restricted to .gov and .mil assets. CAs shall reject all certificate applications containing any FQDNs that are not under the sTLDs for .gov and .mil.

Approval of certificate applications requires successful completion of validation per section 3.2.

In accordance with section 5.5.2, all CAs shall maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. All CAs shall use this information to identify subsequent suspicious certificate requests and may use it as the basis for rejecting a certificate request.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Issuance of a CA Certificate shall require an individual authorized by the CA to deliberately issue a direct command in order for the CA to perform a certificate signing operation. Issuance of a CA certificate shall require written authorization by the FPKIPA.

All Domain Validation TLS Server Authentication certificates and Organizational Validation TLS Server Authentication certificates shall assert a Certificate Transparency (CT) Signed Certificate Timestamp (SCT) in the x509v3 certificate extension. The CA shall submit a pre-certificate to a minimum of two (2) Certificate Transparency Logs for certificates with a validity period less than or equal to 395 days. Information included in the pre-certificates shall not be redacted prior to submission to the CT Logs.

- At least one of the CT Logs shall be a log operated by Google.
- At least one of the CT Logs shall be a log operated by a government or business entity other than Google.

There is no limit on the maximum number of CT Logs which may be submitted to.

The CA shall include at least two (2) SCTs meeting the variety requirements in the x509v3 certificate extension for the Domain Validation TLS Server Authentication certificate or the Organizational Validation TLS Server Authentication certificate issued.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA shall issue the certificate according to the certificate requesting protocol used by the Applicant (this may be automated) and, if the protocol does not provide inherent notification, also notify the Applicant of the issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Failure of the Subscriber to object to a requested certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

As specified in section 2.1, all CA certificates shall be published in repositories.

4.4.3 Notification of certificate issuance by the CA to other entities

CAs shall notify the FPKIPA of CA Certificate issuances.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See section 9.6.3.

The intended scope of usage for a private key shall be in accordance with the Certificate Profiles defined in Appendix D and section 7 of this CP.

4.5.2 Relying party public key and certificate usage

See section 4.9.6

4.6 Certificate renewal

Renewal is defined as the re-issuance of a certificate with no changes to the public key, no changes to the identity information, and a new validity period for the certificate.

4.6.1 Circumstance for certificate renewal

CA certificates shall not be renewed. Domain Validation TLS Server Authentication and Organizational Validation TLS Server Authentication certificates shall not be renewed. Certificate renewal requests shall be treated as new applications and information verified in accordance with section 4.2.1

OCSP Delegated Responder certificates may be renewed.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

The CA shall verify that the OCSP Delegated Responder certificate expiration date shall not exceed 395 days from the date of initial certificate issuance.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

Re-key is defined as the issuance of a certificate with a new public key, no changes to the identity information, and a new validity period for the certificate.

4.7.1 Circumstance for certificate re-key

Certificates under this policy shall not be re-keyed. Certificate re-key requests shall be treated as new applications and information verified in accordance with section 4.2.1.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

Modification is defined as the re-issuance of a certificate with the same public key, same validity period, and changes made to the identity information or information in the certificate such as policies and key usage.

4.8.1 Circumstance for certificate modification

Domain Validation TLS Server Authentication and Organization Validation TLS Server Authentication certificates shall not be modified. OCSP Delegated Responder certificates shall not be modified.

CA certificates may be modified to update attributes other than the public key. A CA certificate shall not be modified to add restrictions not in the original certificate unless all Subscriber certificates previously issued by the CA conform to the new restrictions.

4.8.2 Who may request certificate modification

An authorized representative of either the Root CA or Subordinate CA may request certificate modifications.

4.8.3 Processing certificate modification requests

Certificate issuance by the Root CA shall require an individual authorized by the CA to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. Modification of a CA certificate by the Root CA shall require written authorization by the FPKIPA.

4.8.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA shall revoke a Certificate as rapidly as possible but within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The CA obtains evidence that the Certificate was misused;
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted;
7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
8. The CA is made aware of a material change in the information contained in the Certificate;
9. The CA is made aware that the Certificate was not issued in accordance with this CP or the CA's Certification Practice Statement;
10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
12. The CA's right to issue Certificates under this CP expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
14. Revocation is required by this CP and/or the CA's CPS;
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties; or
16. The CA received a lawful and binding order from a government, judicial or regulatory body to revoke the Certificate.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the CA's CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under this CP expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by this CP and/or the Issuing CA's CPS;
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties; or
11. The CA received a lawful and binding order from a government, judicial or regulatory body to revoke the Certificate.

4.9.2 Who can request revocation

The Subscriber, RA, or CA can initiate revocation of Subscriber or CA certificates. The FPKIPA may also direct any revocation of a CA certificate.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

CAs shall provide a process for Subscribers to request revocation of their own Certificates. The process shall be described in the CA's CPS. The CA shall maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries. A request from Subscribers to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated.

The CA shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for submitting Certificate Problem Reports. The CA shall publicly disclose the instructions through a readily accessible online means.

4.9.4 Revocation request grace period

There is no revocation grace period.

4.9.5 Time within which CA shall process the revocation request

CAs shall revoke certificates as quickly as practical upon receipt of a revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

The CA shall begin investigation of a Certificate Problem Report immediately upon receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement or Inspector General official that a Web site violates U.S. Federal regulation should carry more weight than a complaint from a user alleging that they were unable to complete their transaction); and
4. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

All CAs operating under this policy provide revocation information in accordance with section 4.9.7 and section 4.9.9.

It is recommended that relying parties process the expiration date of the certificate and perform certificate revocation checking, and comply with this information, whenever using a U.S. Federal Public Trust TLS PKI certificate in a transaction.

4.9.7 CRL issuance frequency

For the status of Domain Validation TLS Server Authentication and Organization Validation TLS Server Authentication certificates, CAs shall publish CRLs. CAs shall update and reissue CRLs at least once every 24 hours and the value of the nextUpdate field shall not be more than seven days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates, the root CA shall update and reissue CRLs at least (i) once every 31 days and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field shall not be more than 32 days beyond the value of the thisUpdate field.

4.9.8 Maximum latency for CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9 On-line revocation/status checking availability

OCSP responses shall conform to RFC6960 and/or RFC5019. OCSP responses shall either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by a Delegated OCSP Responder Certificate signed by the CA that issued the Certificate whose revocation status is being checked.

4.9.10 On-line revocation checking requirements

The CA shall support an OCSP capability using the GET method for Certificates.

For the status of Domain Validation TLS Server Authentication and Organization Validation TLS Server Authentication certificates, the CA shall update information provided via OCSP every 24 hours. OCSP responses shall have a maximum expiration time of seven (7) days.

For the status of Subordinate CA Certificates, the root CA shall update information provided via OCSP at least (i) every 31 days and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder shall not respond with a “good” status. The CA shall monitor the responder for such requests as part of its security response procedures.

4.9.11 Other forms of revocation advertisements available

Subscribers may rely on stapling, in accordance with RFC4366, to distribute OCSP responses. The CA shall be responsible for supporting OCSP status responses even if a Subscriber decides to staple OCSP responses.

4.9.12 Special requirements related to key compromise

See section 4.9.1

In the case of a compromise of a CA certificate, the CA must immediately notify the FPKI PA that the CA certificate has been compromised. See section 5.7.1 for incident handling procedures.

4.9.13 Circumstances for suspension

Certificates issued under this policy shall not be suspended.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Revocation entries on a CRL or OCSP Response shall not be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service availability

The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA shall maintain an online Repository 24 hours a day, 7 days a week with a minimum of 99.5% availability overall per year that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA shall maintain a 24 hours a day, 7 days a week ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint

to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Private keys for certificates issued under this policy shall not be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Root CA and Subordinate CAs, and any remote workstations used to perform administration activities for the CAs, except where specifically noted.

5.1.1 Site location and construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, shall:

- Ensure that no unauthorized access to the hardware is permitted.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate for the current mode of operation
- That cryptographic modules are in place when “open,” and secured when “closed”
- Any security containers are properly secured
- Physical security systems are functioning properly
- The area is secured against unauthorized access

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and air conditioning

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power causes a shutdown.

All Repositories shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water exposures

CA equipment shall be installed such that it is not in danger of exposure to water. Potential water damage from fire prevention and protection measures are excluded from this requirement.

5.1.5 Fire prevention and protection

CA equipment shall use facilities equipped with fire suppression mechanisms.

5.1.6 Media storage

Media shall be stored so as to protect it from accidental damage, such as water, fire, or electromagnetic damage. Media shall be stored to protect it from unauthorized physical access.

5.1.7 Waste disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner and rendered unrecoverable.

5.1.8 Off-site backup

Full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week for Subordinate CAs. At least one full backup copy shall be stored at an off-site location separate from CA equipment. Only the latest full backup is required to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

The requirements of this policy are defined in terms of three roles:

1. Administrator
2. Officer
3. Security

These three roles are employed at the CA. Separation of duties shall comply with section 5.2.4, and requirements for two-person control with section 5.2.2, regardless of the titles and numbers of trusted roles.

The Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys
- Routine operation of the CA equipment and operations such as system backups and recovery or changing recording media

Administrators shall not issue certificates to Subscribers.

The Officer shall be responsible for:

- Approving and executing the issuance of the certificates where inspection of the validation information is required
- Requesting, approving and executing the revocation of certificates
- Performing internal self-audits at least every quarter in accordance with section 8.7

The Security trusted role shall be responsible for:

- Reviewing, maintaining, and archiving audit logs
- Overseeing internal compliance and self-audits to ensure that the CA is operating in accordance with its CPS

Each CA shall maintain lists, including names, contact information, and copies of appointment memoranda of those who act in these trusted roles, and shall make them available during audits. The CA shall make this information a part of the permanent records of the CA. However, the CA shall not maintain personnel records or investigative records requiring protection under the Privacy Act.

5.2.2 Number of Individuals Required per Task

The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in the physically secured environment described in 5.1.2.

Where multi-party control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1. Multi-party control shall not be achieved using personnel that serve in the Security trusted role.

5.2.3 Identification and authentication for each role

An individual shall be identified and authenticated before being permitted to perform any actions set forth above for that role or identity. All trusted roles shall use a unique

credential created by or assigned to a single individual for identification and authentication. CAs shall implement multi-factor or multi-party authentication for all Administrator trusted role access to Certificate System Components including operating system and software. All CAs shall implement multi-factor authentication for the Officer trusted role.

5.2.4 Roles requiring separation of duties

Individuals may only assume one of the Administrator, Officer, and Security roles. The CA software and hardware shall identify and authenticate its users and enforce least privilege. The CA software and hardware shall ensure that no user can assume both the Administrator and Officer roles, assume both the Administrator and Security roles, or assume both the Security and Officer roles.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS.

5.3.2 Background check procedures

Trusted role personnel shall, at a minimum, pass a background investigation covering:

- Employment
- Education
- Place of residence
- Law Enforcement
- References

The period of investigation shall cover at least the last five years for each area, excepting the residence check which shall cover at least the last three years. Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 13467 or equivalent.

5.3.3 Training Requirements and Procedures

All individuals in trusted roles shall receive comprehensive training. Training shall be conducted in the following areas:

- Basic Public Key Infrastructure knowledge
- CA security principles and mechanisms
- All trusted role duties

- Disaster recovery and business continuity procedures
- Understanding and knowledge of this CP

The CA shall provide all Officers with additional skills-training that covers:

- Authentication and identity verification policies and procedures including the procedures allowed by this CP and the CA's CPS
- Common threats to the identity verification process including phishing and other social engineering tactics

The CA shall require all Officers to pass an examination provided by the CA on the information verification requirements outlined in this CP and the CA's CPS. The CA shall that ensure that individuals with Officer duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA shall maintain records of training for all individuals in trusted roles. The CA shall document that each individual in a trusted role possesses the skills required by a task before allowing the individual to perform that task.

5.3.4 Retraining Frequency and Requirements

All personnel in trusted roles shall maintain skill levels consistent with the CA's training and performance programs.

All personnel in trusted roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA that are not authorized in this CP, the CA CPS, or other published procedures.

5.3.7 Independent Contractor Controls

Direct contractor personnel employed to operate any part of the CAs or perform functions pertaining to the infrastructure shall be subject to the same personnel requirements set forth in this CP.

5.3.8 Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that trusted role.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The CA shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request, the time and date, any CA Officer roles involved, and the domain validation method used for each FQDN for Domain Validation TLS Server Authentication certificates and Domain Validation TLS Server Authentication certificates. The CA shall make these records available to its Qualified Auditor as proof of the CA's compliance with this CP and the CA's CPS.

The CA shall record CA key lifecycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction
- Cryptographic device lifecycle management events

The CA shall record CA and Subscriber Certificate lifecycle management events, including:

- Certificate requests and revocation requests
- All verification activities stipulated in this CP and the CA's CPS
- Acceptance and rejection of certificate requests
- Issuance of Certificates
- Generation of Certificate Revocation Lists and OCSP entries

The CA shall record Security events, including:

- Successful and unsuccessful PKI system access attempts
- PKI and security system actions performed
- Security profile changes
- Clock adjustments
- System crashes, hardware failures, and other anomalies
- Firewall and router activities
- Entries to and exits from the CA facility

Log entries shall include the following elements:

1. Date and time of entry
2. Identity of the person performing the action if a person is involved in the action
3. Description of the entry

5.4.2 Frequency for Processing and Archiving Audit Logs

Audit logs shall be reviewed at least once every thirty (30) days. Audit log reviews shall include verifying that the logs have not been tampered with, inspecting log entries, and performing a root cause analysis for any alerts or irregularities in the logs.

All significant events and the root cause analysis shall be explained in an audit log summary. Actions taken as a result of the audit log reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained on-site until reviewed, in addition to being archived as described in section 5.5. The Security trusted role shall be responsible for overseeing the migration of audit logs from the CA to the archives.

The CA shall retain any audit logs generated for at least seven years. The CA shall make these audit logs available to its Qualified Auditor upon request.

5.4.4 Protection of Audit Log

The CA shall ensure audit logs are unalterable or maintain an integrity mechanism to identify any changes.

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures shall be implemented to ensure that only authorized people archive or delete security audit data. Procedures shall be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. Copies of the audit logs shall be sent off-site on a monthly basis.

5.4.6 Audit Log Accumulation System (internal vs. external)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g. overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

5.4.7 Notification to event-causing subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability assessments

The CA's security program shall include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate management processes
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate data and Certificate management processes
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats

All CAs shall undergo or perform a Vulnerability Scan:

- At least once per quarter, on public and private IP addresses identified as within the CA's system boundaries
- Within one week of receiving a request from the FPKIPA or the U.S. Government Federal Information Security Modernization Act Authorizing Official for the CA
- After any system or network changes that the CA determines are significant

Subordinate CAs shall undergo a Penetration Test on the CA system boundaries on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant.

CAs shall record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

5.5 Records archival

CAs shall archive records separately from the CA backups. In addition to the archive requirements specified in this CP, archive procedures shall follow either the General Records Schedules established by the National Archives and Records Administration (NARA) or an agency-specific general records schedule as applicable.

5.5.1 Types of records archived

CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate issued by the CA. At a minimum, the following data shall be recorded for archive:

- CA accreditation
- Certificate Policy
- Certification Practice Statement(s)
- Contractual obligations and other agreements concerning operations of the CA
- Security events, as specified in section 5.4.1
- CA key lifecycle management events, as specified in section 5.4.1
- Subscriber Certificate lifecycle management events, as specified in section 5.4.1
- Subscriber agreements and / or Terms of use agreements
- All certificates issued
- All CRLs issued
- Qualified Auditor reports
- Any changes to the Audit parameters
- Appointment of an individual to a trusted role
- Other data or applications to verify archive contents
- All certificate compromise notifications
- Violations of Certificate Policy
- Violations of Certification Practice Statement

5.5.2 Retention period for archive

The CA shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation information thereof, for a minimum of seven years without any loss of data after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

No unauthorized user shall be permitted to write to, modify, or delete the archive records. Records of transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the CA. If the original media cannot retain the data for the required archived period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Alternatively, a CA operating under this policy may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall be maintained for a period that equals or exceeds the archive requirements for the data.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

Archive records maintained in digital format shall be time-stamped as the records are created. The system clocks used for time-stamping shall be maintained in synchrony with an authoritative time standard.

5.5.6 Archive collection system (internal or external)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Key changeovers are not applicable for any CAs operating under this CP and shall not be done. A new CA signing key constitutes a new CA and a new CA Subject Name shall be used.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CAs shall have an Incident Response Plan and a Disaster Recovery Plan. The CA is not required to publicly disclose the Incident Response Plan and Disaster Recovery Plan but shall make the plans available to the CA's Qualified Auditor upon request.

The FPKIPA shall be notified by the CAs operating under this policy of any incident. An incident is defined as a violation or imminent threat of violation of this CP, the CA's CPS, government memorandum of agreements, or any other document that governs the operations of the CA. An incident may include but is not limited to the following:

- CA private key compromise
- Suspected or detected compromise of the CA including the certificate status services required of the CA Repository
- Physical or electronic penetration of the CA including the certificate status services required of the CA Repository
- Successful denial of service attacks on the CA including the certificate status services required of the CA Repository
- Suspected or detected issuance of certificates used for unethical purposes such as (but not limited to) promoting malware or illegal software
- A known or reasonably known, publicly reported compromise of the CA including the certificate status services required of the CA Repository
- Any certificate issuance not in compliance with this CP, this CP's certificate profiles, or the CA's CPS

The CA shall notify the FPKIPA within 24 hours from the time the incident was discovered. An initial security incident report shall be submitted to the FPKIPA and shall include the following information:

1. Which CA was affected by the incident
2. When the incident was discovered
3. How the incident was discovered
4. If available and applicable, any evidence of attribution for the incident
5. The CA's interpretation of the incident
6. A complete list of all certificates that were either mis-issued or not compliant with this CP and the CA's CPS as a result of the incident.

A final security incident report shall be submitted at a date specified by the FPKIPA and shall include the following information:

1. A complete timeline of events
2. A root cause analysis
3. Remediation actions implemented to address the underlying root cause including specific technical or procedural changes, and any updates to the CA's CPS
4. Proof the mis-issued certificates were revoked
5. A statement that the incident has been fully remediated

In coordination with the CA, the FPKIPA may conduct the following activities as part of an incident response:

- Publicly publish a final incident report in one or more internet-accessible locations, with information redacted as necessary
- Report incidents to the individual trust store operator

5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted

When computing resources, software, and/or data are corrupted, CAs shall ensure the system's integrity has been restored before returning to operation.

If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information.

5.7.3 Recovery Procedures after Key Compromise

In the event of a Subordinate CA private key compromise, the following operations shall be performed:

- The FPKIPA shall be immediately notified
- All subscriber certificates shall be revoked within twenty-four (24) hours

- A final long term CRL with a nextUpdate time past the validity period of all issued subscriber certificates shall be generated
- The final CRL shall be available for all relying parties until the validity period of all issued certificates has passed
- The Root CA shall revoke the Subordinate CA certificate within seven (7) days

If the Root Certificate private key is compromised, the CA shall notify the FPKIPA immediately.

In all cases, the CA and the FPKIPA shall initiate procedures to notify subscribers and trust store operators of the compromise.

5.7.4 Business continuity capabilities after a disaster

CAs disaster recovery procedures shall be in place to reconstitute the CA including the certificate status services required of the CA Repository within six (6) hours of failure.

In the case of a disaster whereby the CA installation is damaged and all copies of the CA signature key are destroyed as a result, the FPKIPA shall be notified at the earliest feasible time, and the FPKIPA shall take whatever action it deems appropriate.

5.8 CA or RA termination

This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs and provide OCSP responses until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy.

When a CA operating under this policy terminates operations before all certificates have expired, any issued certificates that have not expired shall be revoked. The CA shall generate a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has expired.

Once the final CRL has been issued, the private signing key(s) of the CA to be terminated shall be destroyed. The terminated CA certificate shall be revoked.

If the terminated CA is the Root CA, the FPKIPA shall notify the trust store operator of the need to remove the Root Certificate from the applicable trust stores.

Prior to CA termination, the CA shall provide archived data to an archive facility.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

The CA shall:

1. Prepare and follow a Key Generation Script
2. Have a Qualified Auditor witness the CA Key Pair generation process or review a video of the entire CA Key Pair generation process
3. Have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair
4. Generate the CA keys in a physically secured environment as described in the CA's CPS
5. Generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge
6. Generate the CA keys within cryptographic modules that meet or exceed FIPS 140 Level 3 validation
7. Log its CA key generation activities
8. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP and CA's CPS and its Key Generation Script

The documentation of the procedure shall be detailed enough to show that appropriate role separation was used and the CA key pair generation shall create a verifiable audit trail that the security requirements for procedures were followed.

6.1.1.2 RA Key Pair Generation

Registration Authorities as a function of the CA shall not generate Subscriber key pairs. Enterprise Registration Authorities as a participant as defined in section 1.3.4 shall not generate Subscriber key pairs.

6.1.1.3 Subscriber Key Pair Generation

Subscribers shall generate their own keys in compliance with Sections 6.1.5 and 6.1.6 and the Subscriber Agreement or Terms of Use.

The CA shall reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key due to Debian weak key (see http://wiki.debian.org/SSLkeys) or a ROCA weak key (see Common Vulnerabilities and Exposures identifier CVE-2017-15361).

6.1.2 Private key delivery to subscriber

Subscribers shall generate their own keys. This section is not applicable.

6.1.3 Public key delivery to certificate issuer

The public key shall be delivered securely to the Issuing CA for certificate issuance. The certificate request process shall ensure that the Applicant possesses the private key associated with the public key presented for certification.

6.1.4 CA public key delivery to relying parties

A Root CA certificate shall be conveyed to trust store operators and relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for the self-signed Root CA certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to trust store operators or relying parties via secure mechanisms
- Secure distribution of the self-signed certificate through secure out-of-band mechanisms
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources
- Secure mechanisms used by the trust store operators to distribute publicly trusted Root CA certificates to relying parties

6.1.5 Key sizes

Certificates shall meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

Digest algorithm	SHA-256
Minimum RSA modulus size (bits)	4096

(2) Subordinate CA Certificates

Digest algorithm	SHA-256
Minimum RSA modulus size (bits)	2048

(3) Subscriber Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

6.1.6 Public key parameters generation and quality checking

For RSA moduli, the CA shall confirm that the value of the public exponent *e* is an odd positive integer such that:

- $2^{16} < e < 2^{256}$

The CA shall perform partial public key validation as specified in Section 5.3.3 of NIST SP 800-89 to confirm that the modulus is an odd number, is not the power of a prime, and has no factors smaller than 752.

For ECC, the CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine as specified in NIST SP 800-56A.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Root CA Private Keys shall not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself
2. Certificates for Subordinate CAs
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates)
4. Certificates for OCSP Response verification

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above shall consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules specified in FIPS 140-2.

Cryptographic modules for CAs, including any cryptographic modules used in certificate status services required of the CA Repository such as OCSP responders, shall be hardware modules validated as meeting FIPS 140-2 Level 3 or above.

Subscribers should use modules validated as meeting FIPS 140-2 Level 1 or above to generate key pairs.

6.2.2 Private key (n out of m) multi-person control

For all CAs:

- A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key
- CA signature keys may be backed up only under at least two-person control
- Access to CA signing keys backed up for disaster recovery shall be under at least two-person control
- The names of the parties used for two-person control shall be made available for inspection during Qualified Audits
- Multi-person control shall not be achieved using personnel that serve in the Security trusted role

There is no stipulation for Subscriber private key multi-person control.

6.2.3 Private key escrow

Private keys shall not be escrowed.

6.2.4 Private key backup

For all CAs:

- The private key shall be backed up under the same multi-person control as the original signature key
- At least one copy of the CA private key shall be stored off-site in a secure storage facility separate from the CA
- All copies of the CA private key shall be accounted for and protected in the same manner as the original
- Backup procedures shall be included in the CA's CPS

Subscriber private keys may be backed up or copied by the Subscriber, but shall be held in the Subscriber's control.

6.2.5 Private key archival

Private keys may be only archived by the parties represented by the Subject identified in the corresponding public key certificate.

6.2.6 Private key transfer into or from a cryptographic module

CAs shall generate their own keys in FIPS 140 validated cryptographic modules, in compliance with sections 6.1.5 and 6.1.6. CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4. At no time shall the CA private key exist in plaintext outside the cryptographic module. Private or symmetric keys used to encrypt other private keys for transport shall be protected from disclosure.

There is no stipulation for Subscriber private key transfers into or from a cryptographic module.

6.2.7 Private key storage on cryptographic module

CAs shall protect their private key in a system or device that has been validated as meeting at least FIPS 140 Level 3.

There is no stipulation for Subscriber private key storage.

6.2.8 Activating Private Keys

For all CAs, private key activation shall implement multiparty control as specified in section 5.2.2.

There is no stipulation for Subscriber private key activation.

6.2.9 Deactivating Private Keys

For all CAs:

- Cryptographic modules that have been activated shall not be available to unauthorized access.
- After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the CA's CPS.
- CA cryptographic modules shall be removed and stored in a secure container when not in use.

There is no stipulation for Subscriber private key deactivation.

6.2.10 Destroying Private Keys

Individuals in trusted roles shall destroy all CA Certificate and Delegated OCSP Responder Certificate private keys when the keys are no longer needed. All CAs shall document the private key destruction methods in the CPS.

There is no stipulation for Subscriber private key destruction.

6.2.11 Cryptographic Module Capabilities

See section 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public key archival

For all CAs, the CA Certificate and public key shall be archived in accordance with section 5.5.1.

There is no stipulation for Subscriber public key archival.

6.3.2 Certificate operational periods and key pair usage periods

Root CA Certificates shall have a Validity Period no greater than 20 years. Subordinate CA Certificates shall have a Validity Period no greater than 10 years. All certificates signed by a CA key pair shall expire before the end of that key pair's usage period.

Domain Validation TLS Server Authentication Certificates and Organization Validation TLS Server Authentication Certificates shall have a Validity Period no greater than 395 days.
Delegated OCSP Responder Certificates shall have a Validity Period no greater than 45 days.

6.4 Activation data

6.4.1 Activation data generation and installation

For all CAs, CA activation data may be user-selected by each of the multiple parties holding that activation data. If the activation data shall be transmitted, it shall be via a channel protected commensurate with the protection supplied by the key itself, and distinct in time and place from the associated cryptographic module.

There is no stipulation for Subscriber activation data.

6.4.2 Activation data protection

For all CAs, this CP makes no further stipulation beyond that specified in FIPS 140.

There is no stipulation for Subscriber activation data.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Administrator privileges to all Certificate System Components shall only be granted to the Administrator trusted role. All CAs shall implement multi-factor or multi-party authentication for all Administrator trusted role access to Certificate System Components including operating system and software.

All CAs shall implement multi-factor authentication for the Officer trusted role.

For all CAs and Certificate System Components including certificate status services, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Certificate System Components shall include the following functionality:

- Be configured to remove or disable all accounts, applications, services, protocols, and ports that are not used in the CA's operations
- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles and implement least privilege controls
- Generate and archive audit records for all transactions (see section 5.4)
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Generate and archive audit records for all transactions (see section 5.4)
- Enforce domain integrity boundaries for security critical processes
- Configure workstations with inactivity time-outs to enforce account log out or lock the workstation when no longer in use

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

The system development controls for all CAs and Certificate System Components functions listed below are required:

- The CA hardware and software shall be dedicated to performing one task: the CA
- There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the CA operation
- Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g. by ensuring the random selection of material at time of purchase or installation)
- Hardware and software shall be similarly limited and scanned for malicious code on first use and continuously thereafter

6.6.2 Security management controls

The security management controls for all CAs and all Certificate System Components listed below shall be implemented:

- Configurations, modifications, and upgrades shall be documented and controlled
- Configurations shall be reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.
- There shall be a mechanism for detecting unauthorized modification to the software or configuration
- All system accounts and trusted role accounts shall be reviewed at least every ninety (90) days, and any account that is no longer in use or necessary for operations shall be deactivated
- A process shall be implemented that disables physical and logical access to a Certificate Systems by any trusted role within 24 hours upon termination of the individual's employment or contracting relationship with the CA
- All authentication credentials for any account or trusted role on a Certificate Systems shall be changed whenever authorization to access the account is changed or revoked
- All system accounts and trusted role accounts shall have be configured to lockout access after five (5) failed access attempts
- There shall be an automated mechanism to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events

6.6.3 Life cycle security controls

The security management controls for all CAs and Certificate System Components listed below shall be implemented:

- Hardware and software shall be scanned for vulnerabilities at least every thirty (30) days
- High vulnerabilities shall be patched within sixty (60) days or less
- Critical vulnerabilities shall be patched within ninety-six (96) hours of the discovery of a critical vulnerability not previously addressed

If remediation of a critical vulnerability within ninety-six (96) hours is not possible, the CA shall create and implement a plan to mitigate the vulnerability or document the factual basis for a risk determination that the vulnerability does not require remediation.

For Subordinate CAs, and the Root CA Repository and system support services, penetration testing shall be performed at least every 365 days, and after infrastructure of application upgrades or modifications that the CA determines are significant.

6.7 Network security controls

Secure Zones are a physical or logical separation of Certificate Systems while a High Security Zone is a physical area where a private key or cryptographic equipment is stored. Each Zone is protected commensurate with its level of assurance. A High Security Zone may exist within a Secure Zone that is physically or logically separated from other Secure Zones.

For the Root CA, the CA shall be operated in a High Security Zone and in an offline (powered off, disconnected) or air-gapped (powered on, disconnected) state from all other networks.

For all CAs and Certificate System Components, the network security controls listed below are required:

- Secure Zones shall be implemented to secure Certificate Systems based on functional, logical, and physical (including location) relationships.
- The same security controls shall be applied to all systems co-located in the same Zone with a Certificate System.
- Security support systems shall be configured to protect systems and communications between systems inside Secure Zones and High Security Zones as well as Public Networks (Internet).
- Only trusted roles shall have access to Secure and High Security Zones.
- A network guard or firewall shall protect network access to CA equipment, and limit services allowed to and from the CA equipment to those required to perform CA functions.
- Protection of CA equipment shall be provided against known network attacks.
- All unused network ports and services shall be turned off.
- Any network software present shall be necessary to the functioning of the equipment.
- Any boundary control devices used to protect the network on which equipment is hosted shall deny all but the necessary services to the equipment.
- Repositories, certificate status services, and remote workstations used to administer the CAs shall employ appropriate network security controls.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA. Remote connections shall be restricted, except when:

- The remote connection originates from a device owned by the CA and from a pre-approved IP address. - The connection is through a temporary, non-persistent and encrypted channel that is supported by multi-factor authentication.

6.8 Time-stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificates issued by a CA under this policy shall conform to the Certificate Profiles included as Appendix D.

7.1.1 Version number(s)

Certificates shall be of type X.509 v3.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

Rules for the certificate content and extensions are included as Appendix D.

CAs shall not issue a Certificate with: - Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network) - Semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA

A Precertificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a “certificate” subject to the requirements of RFC 5280 under this CP.

7.1.3 Algorithm object identifiers

The Certificate Profiles in Appendix D describe algorithms used in signing certificates and algorithms for the subject public key information, aligned with section 6.1.5.

Signature Algorithm	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha384WithRSAEncryption	1.2.840.113549.1.1.12
sha512WithRSAEncryption	1.2.840.113549.1.1.13

Public Key Algorithm	Object Identifier
rsaEncryption	1.2.840.113549.1.1.1
ecPublicKey	1.2.840.10045.2.1

7.1.4 Name forms

7.1.4.1 Issuing CA Certificate Subject

The content of the Certificate Issuer Distinguished Name field shall match the Subject Distinguished Name of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

CA Subject Distinguished Name shall conform to PrintableString string type in ASN.1 notation.

7.1.4.2 Subject Information for Standard Server Authentication certificates

By issuing the Certificate, the CA represents that it followed the procedure set forth in this CP and the CA CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

CAs shall not include a Domain Name in a Subject attribute except as validated under section 3.2.2.4.

7.1.4.3. Subject Information - Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in this CP and the CA's CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.5 Name constraints

All Subordinate CA Certificates shall be Technically Constrained. For a Subordinate CA Certificate to be considered Technically Constrained, the certificate shall include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId shall not appear within this extension.

The Subordinate CA Certificate(s) shall include the id-kp-serverAuth extended key usage, and the Subordinate CA Certificate(s) shall include the Name Constraints X.509v3 extension with constraints on dNSName as follows:

- Shall include at least one dNSName in permittedSubtrees
- The permittedSubtrees for dNSName shall be within the constraints of the sTLDs for .gov and .mil

- The permittedSubtrees for dNSName shall not contain any other dnsName ranges outside of the the .gov or .mil sTLDs

For ipAddress, Subordinate CAs shall not issue subscriber certificates with an iPAddress. The Subordinate CA Certificate shall:

- Specify the entire IPv4 and IPv6 address ranges in excludedSubtrees
- Include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0)
- Include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0)

For DirectoryName, the Subordinate CA certificates shall not have DirectoryName present in Name Constraints.

A decoded example for issuance to the domain and sub domains of .mil by a Subordinate CA would be:-

X509v3 Name Constraints:
Permitted:
DNS:mil
Excluded:
IP:0.0.0.0/0.0.0.0
IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

A decoded example for issuance to the domain and sub domains of both .gov and .mil by a Subordinate CA would be:

X509v3 Name Constraints:
Permitted:
DNS:mil
DNS:gov
Excluded:
IP:0.0.0.0/0.0.0.0
IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

7.1.6 Certificate policy object identifier

7.1.6.1. Reserved Certificate Policy Identifiers

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.

The following Certificate Policy identifiers are registered under the National Institute of Standards and Technology (NIST) Computer Science Object Registory (CSOR) OID arc

and reserved for use by the U.S. Government for this CP. These Certificate Policy Identifiers are a required means of asserting compliance with this CP as follows:

- Domain Validated:
  - { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) arcfbca-policies(3) domain-validated(43) } (2.16.840.1.101.3.2.1.3.43),
  - if the Certificate complies with this CP but lacks Subject Identity Information that is verified in accordance with section 3.2.2.1 or section 3.2.3.
- Organization Validated:
  - {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) arcfbca-policies(3) organization-validated(44)} (2.16.840.1.101.3.2.1.3.44),
  - If the Certificate complies with this CP and includes Subject Identity Information that is verified in accordance with section 3.2.2.1.

The following Certificate Policy identifiers are registered under the CAB Forum and reserved for use. These Certificate Policy Identifiers are a required means of asserting compliance with the CAB Forum Baseline Requirements as follows:

- Domain Validated:
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1),
  - If the Certificate complies with the Baseline Requirements but lacks Subject Identity Information that is verified in accordance with section 3.2.2.1 or section 3.2.3
- Organization Validated:
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2),
  - If the Certificate complies with the Baseline Requirements and includes Subject Identity Information that is verified in accordance with section 3.2.2.1.

If the Certificate asserts the policy identifiers for Domain Validated, then the certificate shall not include organizationName and stateOrProvinceName in the Subject field. If the Certificate asserts the policy identifiers for Organization Validated, then the certificate shall include organizationName, stateOrProvinceName and countryName in the Subject field.

7.1.6.2. Root CA Certificates

A Root CA Certificate shall not contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

All Subordinate CA's shall be an Affiliate as defined in this CP.

A Certificate issued to a Subordinate CA shall shall contain in the Certificate's certificatePolicies extension:

1. One of more of the US Government reserved policy object identifiers defined in section 7.1.6.1 to indicate the Subordinate CA's compliance with this CP, and
2. One or more of the CAB Forum reserved policy object identifiers in section 7.1.6.1 to indicate the Subordinate CA's compliance with the CAB Forum Baseline Requirements

7.1.6.4 Subscriber Certificates

A Domain Validation TLS Server Authentication Certificates or Organization Validation TLS Server Authentication Certificates issued to a Subscriber shall contain in the Certificate's certificatePolicies extension:

1. One US Government reserved policy object identifiers defined in section 7.1.6.1 that indicates adherence to and compliance with this CP
2. One of the CAB Forum reserved policy object identifiers defined in section 7.1.6.1 that indicates adherence to and compliance with the CAB Forum Baseline Requirements

The certificates shall contain certificate policy identifier(s) for either Domain Validated policies or Organization Validated policies but shall not assert certificate policy identifiers for both.

The CA shall document in its CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the CAB Forum Baseline Requirements and this CP.

Delegated OCSP Responder Certificates shall contain all the certificate policy OIDs defined in section 7.1.6.1 for all certificates issued by the CA and covered by the OCSP responses.

7.1.7 Usage of Policy Constraints extension

Subordinate CA certificates may assert policy constraints.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP may contain policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2 CRL profile

Certificate Revocation Lists (CRLs) created by a CA under this policy shall conform to the Certificate Revocation List extensions profile included as Appendix D.

7.2.1 Version number(s)

The CAs shall issue X.509 version two (v2) CRLs.

7.3 OCSP profile

OCSP Responses under this policy shall conform to the OCSP Response profile included as Appendix D.

7.3.1 Version number(s)

OCSP responses operated under this policy shall use OCSP version 1.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The CAs operated under this CP are Technically Constrained (see section 7.1.5). CAs shall be audited in accordance with section 8.7.

The period during which the CA issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period shall not exceed one year in duration.

Before issuing Subscriber certificates or Subordinate CA certificates, any CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in section 8.4. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 Identity/qualifications of assessor

CA audits shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit

2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see section 8.4)
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
4. For audits conducted in accordance with the WebTrust standard, licensed by WebTrust
5. Bound by law, government regulation, or professional code of ethics, and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's relationship to assessed entity

The Qualified Auditor either shall be a private firm that is independent from the CA being audited, or it shall be sufficiently organizationally separated from the CA to provide an unbiased, independent evaluation. An example of the latter situation may be a Federal agency Inspector General. To insure independence and objectivity, the Qualified Auditor may not have served the CA in developing or maintaining the CPS. The FPKIPA shall determine whether the Qualified Auditor meets the requirements for independence and objectivity.

8.4 Topics covered by assessment

The CAs shall undergo an audit in accordance with all of the following:

1. WebTrust for Certification Authorities, Version 2.0 or later
2. WebTrust for Certification Authorities - SSL Baseline with Network Security, Version 2.2 or later
3. Compliance of the CA's CPS against this CP

Audits shall incorporate periodic monitoring and/or accountability procedures to ensure that the audits continue to be conducted in accordance with the requirements of the scheme. The audit shall be conducted by a Qualified Auditor, as specified in section 8.3.

8.5 Actions taken as a result of deficiency

When the Qualified Auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the CAs, the following actions shall be performed:

- The Qualified Auditor shall note the discrepancy
- The Qualified Auditor shall notify the CA promptly
- The CA shall propose a remedy, including expected time for completion, to the FPKIPA

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may decide to temporarily halt operation of the CA, to revoke a certificate issued to the CA, or take other actions it deems appropriate.

8.6 Communication of results

The Audit Letter shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in section 7.1.6.1.

The Audit Letter shall include:

- Name and address of the organization performing the audit
- Name of the auditor(s)
- Distinguished name and SHA256 fingerprint of each CA that was included in the audit
- Audit criteria, with version number, that was used to audit each of the CAs
- A list of the CA policy documents, with version numbers, referenced during the audit
- Whether the audit is for a period of time or a point in time
- For a period of time audit: the start and end date of the period
- For a point in time audit: the point-in-time date
- The date the Audit Letter was issued

The CA shall make the Audit Letter publicly available. The CA shall make its Audit Letter publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by the FPKIPA or an Application Software Supplier, the CA shall provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA shall monitor adherence to this CP and the CA's CPS and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

During the period in which a Subordinate CA issues Certificates, the Root CA shall monitor adherence to this CP and the Subordinate CA's CPS. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP requirements are met.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

Section 2 of this policy requires that Repositories including CA Certificates are publicly available. CAs operating under this policy shall not charge additional fees for access to CA Certificates.

9.1.3 Revocation or status information access fees

Section 2 of this policy requires that Repositories including certificate status services (CRLs and OCSP) are publicly available. CAs operating under this policy shall not charge additional fees for access to CRLs and OCSP services.

CAs shall not charge Subscribers a fee to revoke a certificate.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

CA information not requiring protection shall be made publicly available.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

A CA shall not disclose non-certificate information to any third party unless authorized by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S. court of competent jurisdiction. The contents of the archives maintained by CAs operating under this policy shall not be released except as required by this policy, required by U.S. law, U.S. government rule or regulation, or order of a U.S court of competent jurisdiction. The FPKI Policy Authority must authenticate any request for release of information.

9.4 Privacy of personal information

9.4.1 Privacy plan

CAs shall conduct a Privacy Threshold Assessment, and implement and maintain any required Privacy Impact Assessments and Privacy Plans in accordance with the requirements of the Privacy Act of 1974, as amended.

9.4.2 Information treated as private

The CAs shall protect any subscriber personally identifying information from unauthorized disclosure.

Records of individual transactions may be released upon request of any subscribers.

9.4.3 Information not deemed private

Information included in certificates and certificate status information are not private information and are not subject to the protections outlined in section 9.4.2.

9.4.4 Responsibility to protect private information

Sensitive information shall be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and consent to use private information

The CA is not required to provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations of section 9.4.

9.4.6 Disclosure pursuant to judicial or administrative process

The FPKIPA or CAs shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

9.4.7 Other information disclosure circumstances

None.

9.5 Intellectual property rights

The FPKIPA and CAs shall not knowingly violate intellectual property rights held by others.

9.6 Representations and warranties

9.6.1 CA representations and warranties

CAs shall warrant that their procedures are implemented in accordance with this CP and that all certificates issued were issued in accordance with the stipulations of this policy.

A CA that issues certificates under this policy shall conform to the stipulations of this policy, including:

- Providing to the FPKIPA a CPS, as well as any subsequent changes, for conformance assessment
- Ensuring a Terms of Service or Subscriber Agreement is agreed to with the Subscribers
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificates
- Maintaining evideence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2 RA representations and warranties

An RA, as the party described in section 1.3.4, may perform registration functions as described in this policy. An RA shall comply with the stipulations of this policy, and comply with the CA CPS approved by the FPKIPA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber representations and warranties

The CA shall require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

A Subscriber shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. The Subscriber Agreement or Terms of Use shall require the Subscriber to:

- Provide accurate and complete information in the transactions with the CA
- Protect the private key(s) at all times, in accordance with this policy
- Promptly notify the CA upon suspicion of loss or compromise of the private key(s)
- Cease use of the private key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s)
- Use certificates provided by the CA's only for transactions related to U.S. Government business

The CA may use an electronic or "click-through" agreements provided that the CA has determined that such agreements are legally enforceable. A separate agreement may be used for each certificate request, or a single agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

9.6.4 Relying party representations and warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8 Limitations of liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This CP becomes effective when approved by the FPKIPA. This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the FPKIPA.

9.10.3 Effect of termination and survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual notices and communications with participants

The FPKIPA shall establish appropriate procedures for communications with CAs operating under this policy via memoranda of agreement as applicable.

9.12 Amendments

9.12.1 Procedure for amendment

The FPKIPA shall review and update this Certificate Policy at least every 365 days.

The review and update shall include any changes needed to address source requirements, including but not limited to:

- U.S. Federal Government mission needs and changes to support the missions
- Baseline Requirements
- Trust store operator requirements

- Browser software vendor requirements

The FPKIPA is responsible for monitoring source requirements, and initiating necessary changes to ensure continued compliance within the required timeframes. After review and approval, the CP document version number and a dated changelog entry shall be added even if no changes were made to the document.

Errors, updates, or suggested changes to this CP can be communicated to the contact in section 1.5.2. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification mechanism and period

Proposed changes to this CP shall be distributed electronically to FPKIPA members and observers in accordance with the Charter and By-laws, and posted publicly for review by any interested party. The FPKIPA shall make any subsequent changes publicly available within 30 days of approval (see section 2.3).

9.12.3 Circumstances under which OID shall be changed

No stipulation.

9.13 Dispute resolution

The FPKIPA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy. If a dispute is between U.S. Federal government entities, and the FPKIPA is unable to facilitate resolution, dispute resolution may be escalated to the White House Office of Management and Budget or to the U.S. Department of Justice, Office of Legal Counsel as necessary.

9.14 Governing law

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation).

9.15 Compliance with applicable law

All CAs operating under this policy are required to comply with applicable law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

Appendix A: Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Air-Gapped: Certificate Systems or components that are physically and logically disconnected from other networks.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Letter: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an audited entity's processes and controls comply with the mandatory provisions of the Baseline Requirements, this Certificate Policy and the Certification Practice(s) Statements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA shall remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Port: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CAB Forum (http://www.cabforum.org).

Certification Authority Authorization: From RFC 6844 (http:tools.ietf.org/html/rfc6844): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.”

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA’s possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate System: The system used by a CA in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI related services.

Certificate System Component: An individual element of a larger Certificate System used to process, approve issuance of, or store certificates or certificate status information.

This includes the database, database server, storage devices, certificate hosting services, registration authority systems, and any other element used in certificate management.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Transparency (CT): Publicly operated record of certificate issuance.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Effective Date: The date, as specified in section 1.2.1, by which entities need to conform to the specified revision of this policy.

Embedded SCT: An SCT delivered via an X.509v3 extension within the certificate.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

High Security Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the CA's Private Key or cryptographic hardware.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its

value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair **.**

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standingin a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Offline: An air-gapped Certificate System or component that is only turned on to conduct certificate activity (i.e. issue / revoke a certificate, issue certificate revocation list, etc).

Online: Certificate Systems or components that are physically and logically connected to the public and/or a private internet.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. The protocol is defined in RFC 6960. See also OCSP Responder.

**Pre-Certificate: An X.509 object constructed from the certificate intended to be issued and submitted to Certificate Transparency logging services, to receive a signed certificate timestamp (SCT). A Pre-certificate is define in RFC 6962.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of section 8.2.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved: - http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml - http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Security Support Systems: A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.

Signed Certificate Timestamp (SCT): A timestamp and promise from a Certificate Transparency operator to add the submitted certificate to the log within a specified time period.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Test Certificate: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no Certificate paths/chains to a root Certificate subject to this Certificate Policy or the Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by the Baseline Requirements, this Certificate Policy and the Certification Practice(s) Statements under which a CA operates.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

Wildcard Certificate: A Domain Name consisting of a single asterisk character followed by a single full stop character (“*.”) followed by a Fully-Qualified Domain Name.

Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

Appendix B: Acronyms

Acronym	Meaning
ACME	Automated Certificate Management Environment
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CT	Certificate Transparency
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SCT	Signed Certificate Timestamp
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security

Appendix C: References

Automatic Certificate Management Environment (ACME), https://datatracker.ietf.org/doc/draft-ietf-acme-acme/

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services – Practices and policy framework.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

NIST SP 800-56-A, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

RFC5752, Request for Comments: 5752, Multiple Signatures in Cryptographic Message Syntax (CMS), Turner et al, January 2010.

RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, et al, January 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency, Laurie, et al, June 2013.

WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

Appendix D: Certificate Profiles

This section specifies the X.509 version 3 certificate profiles, version 2 Certificate Revocation List (CRL) profile, and Online Certificate Status Protocol (OCSP) Response profile for the U.S. Federal Public Trust TLS PKI Certificate Policy. In cases where the profiles and section 7 of this CP are in conflict, section 7 takes precedence and is authoritative.

Certificates issued under this policy are categorized as CA Certificates or Subscriber Certificates. This Certificate Policy defines five (5) different types of certificates (See section 1.1.3) and four associated certificate profiles.

Category	Certificate Type	Profile
CA Certificate	Root CA Certificate	Self-Signed Root CA Certificate Profile
CA Certificate	Subordinate CA Certificate	Subordinate CA Certificate Profile
Subscriber Certificate	Domain Validation TLS Server Authentication Certificates	Server Authentication Certificate Profile
Subscriber Certificate	Organization Validation TLS Server Authentication Certificates	Server Authentication Certificate Profile
Subscriber Certificate	Delegated OCSP Responder Certificates	Delegated OCSP Responder Certificate Profile

There are two profiles covering the Certificate Revocation Lists and OCSP Responses.

Type	Profile
Certificate Revocation Lists	CRL Profile
Online Certificate Status Protocol (OCSP) Responses	OCSP Response Profile

Self-Signed Root CA Certificate Profile

Field	Value and Requirements
Serial Number	Serial number shall be a unique positive integer with a minimum of 64 bits (minimum of 8 octets), not to exceed 20 octets.
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}

Issuer Distinguished Name	Root CA Certificate Issuer Distinguished Name (DN) shall be a unique X.500 DN as specified in Section 7.1.4 of this CP. Distinguished Name shall conform to PrintableString string type in ASN.1 notation. The Root CA Certificate DN shall be: cn=US Federal TLS Root CAx, o=U.S. Government, c=US where "x" is not used for the first Root CA certificate name and is a numeric value that starts at 2 and increments by 1 for any future Root CA certificate Common Names(cn). All non-production Root CA DNs shall include "Test" in the Common Name (cn). A non-production DN example is: cn=US Federal Test TLS Root CA, o=U.S. Government, c=US
Validity Period	Validity Period dates shall be encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter Validity Period shall be no longer than 20 years from date of issue.
Subject Distinguished Name	Subject Distinguished Name (DN) shall match the Issuer DN.
Subject Public Key Information	4096 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}

Extension	Required	Critical	Value and Requirements
subjectInfoAccess	Mandatory	False	id-ad-caRepository (1.3.6.1.5.5.7.48.5): At least one instance of this access method shall be included. All instances of this access method shall include the HTTP URI name form to specify an HTTP accessible location containing a BER or DER encoded "certs-only" CMS message as specified in [RFC5272].
basicConstraints	Mandatory	True	cA=True The pathLenConstraint field shall not be present.
subjectKeyIdentifier	Mandatory	False	Octet String Derived using SHA-1 hash of the public key
keyUsage	Mandatory	True	Bit positions for keyCertSign and cRLSign shall be set.

Extension	Required	Critical	Value and Requirements
			If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit shall also be set.

Subordinate CA Certificate Profile

Field	Value
Serial Number	Serial number shall be a unique positive integer with a minimum of 64 bits (minimum of 8 octets), not to exceed 20 octets. Serial numbers shall be non-sequential.
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	Validity Period dates shall be encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter Validity Period shall be no longer than 10 years from date of issue.
Subject Distinguished Name	Subordinate CA Certificate Subject Distiguished Name (DN) shall be a unique X.500 DN as specified in Section 7.1.4 of this CP. Distinguished Name shall conform to PrintableString string type in ASN.1 notation. The Subordinate CA Certificate DN shall be of the following format: cn=US Federal TLS CAx, o=U.S. Government, c=US Where *x* starts at 1 and is incremented by 1 for each Subordinate CA signed by the Root CA. All other attributes, for the CA Certificate Subject fields, shall not be included. Non-production Subordinate CAs signed by non-production Root CA certificates shall include “Test” in the DN. A non-production DN example is: cn=US Federal Test TLS CA1, o=U.S. Government, c=US Subject name shall be encoded exactly as it is encoded in the issuer field of certificates issued by the subject.
Subject Public Key Information	At least 2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}

Extension	Required	Critical	Value and Requirements
authorityKeyIdentifier	Mandatory	False	Octet String Derived using the SHA-1 hash of the Issuer's public key in accordance with RFC 5280. Shall match SKI of issuing CA.
basicConstraints	Mandatory	True	cA=True The pathLenConstraint field shall be present and set to zero (0).
subjectKeyIdentifier	Mandatory	False	Octet String Derived using SHA-1 hash of the public key
keyUsage	Mandatory	True	Bit positions for keyCertSign and cRLSign shall be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit shall also be set.
extkeyUsage	Mandatory	False	This extension is required for Technically constrained nameConstraints per Section 7.1.2.2 and Section 7.1.5. Required Extended Key Usage: Server Authentication id-kp-serverAuth {1.3.6.1.5.5.7.3.1} Optional Extended Key Usage: Client Authentication id-kp-clientAuth {1.3.6.1.5.5.7.3.2} Other values may be present consistent with use for server authentication, with approval by the FPKIPA.
certificatePolicies	Mandatory	False	See Section 7.1.6.3. At least one US Government certificate policy OID listed in Section 7.1.6.1 asserting compliance with this CP, and one CAB Forum certificate policy OID listed in Section 7.1.6.1 asserting compliance with the CAB Forum Baseline Requirements. The certificate shall include all the

Extension	Required	Critical	Value and Requirements
			certificate policy OIDs for all certificates issued by the CA.
subjectAltName	Optional	False	
authorityInformationAccess	Mandatory	False	OCSP: Publicly accessible URI of Issuing CA's OCSP responder accessMethod = {1.3.6.1.5.5.7.48.1} At least one instance of the OCSP responder access method shall be included. All instances of this access method shall include the HTTP URI name form. id-ad-caIssuers: Publicly accessible URI of Issuing CA's certificate accessMethod = {1.3.6.1.5.5.7.48.2} All instances of this access method shall include the HTTP URI name form to specify an HTTP accessible location containing either a single DER encoded certificate, or a BER or DER encoded "certs-only" CMS message as specified in [RFC5272].
cRLDistributionPoints	Mandatory	False	At least one instance shall be included and shall specify a HTTP URI to the location of a publicly accessible CRL. All URIs included shall be publicly accessible and shall specify the HTTP protocol only. The reasons and cRLIssuer fields shall be omitted.
nameConstraints	Mandatory	True	See Section 7.1.5.

Server Authentication Certificate Profile

This profile for Server Authentication Certificates contains two (2) certificate types:

- *Domain Validation* TLS Server Authentication Certificates
- *Organization Validation* TLS Server Authentication Certificates

There are two (2) differences in the certificate profile implementations between Domain Validation and Organization Validation. The differences are in the *Subject Identity Information* and the *Certificate Policies*.

Field or Extension	Domain Validation	Organization Validation
Subject Identity Information	cn=<one domain name>[,c=US]	cn=<one domain name>,S=District of Columbia,O=U.S.Government,c=US
Certificate Policies	Asserts both the US Government and CAB Forum policy oid for Domain Validation	Asserts both the the US Government and CAB Forum policy oid for Organization Validation

Below is the full server authentication certificate profile with *all* fields and extensions.

Field	Value and Requirements
Serial Number	Serial number shall be a unique positive integer with a minimum of 64 bits (minimum of 8 octets), not to exceed 20 octets. Serial numbers shall be non-sequential.
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	Validity Period dates shall be encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter Validity Period shall be no longer than 395 days from date of issue.
Subject Distinguished Name	Geo-political SDNs: CN (required) shall contain a Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension Organization Name, and State or Province (optional): If present, shall contain both Organization Name, and State or Province. organizationName shall be U.S. Government, and StateorProvince shall be District of Columbia. Country (required) and shall be c=US All other attributes, for the subject field, shall not be included.
Subject Public Key Information	Public key algorithm associated with the public key. May be either RSA or Elliptic curve. rsaEncryption {1.2.840.113549.1.1.1} Elliptic curve key {1.2.840.10045.2.1} **Parameters:** For RSA, parameters field is populated with NULL.

Field	Value and Requirements
	For ECC Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78-1: Curve P-256 {1.2.840.10045.3.1.7} Curve P-384 {1.3.132.0.34} Curve P-521 {1.3.132.0.35} For RSA public keys, modulus must be 2048, 3072, or 4096 bits. Public exponent *e* shall be an odd positive integer such that 2^16+1 < =*e* < 2^256-1.
Issuer Signature	sha256 WithRSAEncryption {1.2.840.113549.1.1.11}

Extension	Required	Critical	Value and Requirements
Authority Key Identifier	Mandatory	False	Octet String Derived using the SHA-1 hash of the Issuer's public key in accordance with RFC 5280. Must match SKI of issuing CA Certificate
basicConstraints	Mandatory	True	cA=False
Subject Key Identifier	Mandatory	False	Octet String Derived using SHA-1 hash of the public key in accordance with RFC 5280
Key Usage	Mandatory	True	**Required Key Usage:** digitalSignature **Optional Key Usage:** keyEncipherment for RSA Keys keyAgreement for Elliptic Curve **Prohibited Key Usage:** keyCertSign and cRLSign
Extended Key Usage	Mandatory	False	**Required Extended Key Usage:** Server Authentication id-kp-serverAuth {1.3.6.1.5.5.7.3.1} **Optional Extended Key Usage:** Client Authentication id-kp-clientAuth {1.3.6.1.5.5.7.3.2} **Prohibited Extended Key Usage:**

Extension	Required	Critical	Value and Requirements
			anyEKU EKU {2.5.29.37.0} all others
Certificate Policies	Mandatory	False	**Required Certificate Policy Fields:** See Section 7.1.6.4. One US Government certificate policy OID listed in Section 7.1.6.1 asserting compliance with this CP, and one CAB Forum certificate policy OID listed in Section 7.1.6.1 asserting compliance with the CAB Forum Baseline Requirements. **Optional Certificate Policy Fields:** certificatePolicies:policyQualifiers policyQualifierId id-qt 1 qualifier:cPSuri
Subject Alternative Name	Mandatory	False	This extension shall contain at least one entry. Each entry shall be a dNSName containing the Fully-Qualified Domain Name of a server. This extension shall not include any Internal Name values. All entries shall be validated in accordance with Section 3.2.2.4.
Authority Information Access	Mandatory	False	**Required AIA Fields:** **OCSP** Publicly accessible URI of Issuing CA's OCSP responder accessMethod = {1.3.6.1.5.5.7.48.1} **Id-ad-calssuers** Publicly accessible URI of Issuing CA's certificate accessMethod = {1.3.6.1.5.5.7.48.2} All instances of this access method shall include the HTTP URI name form to specify an HTTP accessible location containing either a single DER encoded certificate, or a BER or DER encoded "certs-only" CMS

Extension	Required	Critical	Value and Requirements
			message as specified in [RFC5272].
CRL Distribution Points	Mandatory	False	At least one HTTP URI to the location of a publicly accessible, full and complete CRL. The reasons and cRLIssuer fields must be omitted.
Private Extensions	Optional	False	Only extensions that have context for use on the public Internet are allowed. Private extensions must not cause interoperability issues. CA must be aware of and defend reason for including in the certificate, and use of Private Extensions shall be approved by the FPKI Policy Authority.
Transparency Information	Mandatory	False	Must include two or more SCTs or inclusion proofs. From RFC 6962, contains one or more “TransItem” structures in a “TransItemList”.

Delegated OCSP Responder Certificate Profile

Field	Value and Requirements
Version	V3 (2)
Serial Number	Must be a unique positive integer with a minimum of 64 bits (minimum of 8 octets), not to exceed 20 octets
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Distinguished Name of the Issuing CA for the OCSP responder certificate
Validity Period	Encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter No longer than 45 days from date of issue.
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP. The commonName (CN) shall include an indicator of the certificate subject as an OCSP Responder. Organization Name (required) and shall contain U.S. Government (o=U.S. Government) Country (required) and shall be c=US Each X.500 DN is a printableString where possible and contains a single attribute type and attribute value tuple. Example: cn=OCSP Signing Certificate 1, o=U.S. Government, c=US
Subject Public Key Information	rsaEncryption {1 2 840 113549 1 1 1} For RSA, parameters field is populated with NULL. For RSA public keys, modulus shall be 2048, 3072, or 4096 bits. Public exponent *e* shall be an odd positive integer such that 2^16+1 < =*e* < 2^256-1.
Issuer Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}

Extension	Required	Critical	Value and Requirements
Authority Key Identifier	Mandatory	False	Octet String Derived using the SHA-1 hash of the Issuer's public key in accordance with RFC 5280. Must match SKI of issuing CA Certificate
Subject Key Identifier	Mandatory	False	Octet String 20 byte SHA-1 hash of the binary DER encoding of the OCSP responder public key in accordance with RFC 5280

Extension	Required	Critical	Value and Requirements
Key Usage	Mandatory	True	**Required Key Usage:** digitalSignature **Prohibited Key Usage:** All others
id-pkix-ocsp-nocheck {1.3.6.1.5.5.7.48.1.5}	Mandatory	False	Null
Extended Key Usage	Mandatory	True	**Required Extended Key Usage:** id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9} **Prohibited Extended Key Usage:** All others, including anyEKU EKU {2.5.29.37.0}
Certificate Policies	Mandatory	False	**Required Certificate Policy Fields:** See Section 7.1.6.4. The certificate shall include all the certificate policy OIDs for all certificates issued by the CA and covered by the OCSP responses. **Optional Certificate Policy Fields:** certificatePolicies:policyQualifiers policyQualifierId id-qt 1 qualifier:cPSuri
Authority Information Access	Optional	False	**Required AIA Fields:** **Id-ad-calssuers** Publicly accessible URI of Issuing CA's certificate accessMethod = {1.3.6.1.5.5.7.48.2} All instances of this access method shall include the HTTP URI name form to specify an HTTP accessible location containing either a single DER encoded certificate, or a BER or DER encoded "certs-only" CMS message as specified in [RFC5272].

CRL Profile

Field	Value and Requirements
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Distinguished Name of the CA Issuer
thisUpdate	Encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter See Section 4.9.7 for publishing intervals.
nextUpdate	Encoded as UTCTime for dates through 2049 and GeneralizedTime for dates thereafter See Section 4.9.7 for validity period intervals.
Revoked Certificates List	0 or more 2-tuple of certificate serial number and revocation date (Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
Issuer Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}

CRL Extension	Required	Critical	Value
CRL Number	Mandatory	False	Monotonically increasing integer (never repeated)
Authority Key Identifier	Mandatory	False	Octet String: Derived using the SHA-1 hash of the Issuer's public key in accordance with RFC 5280. Shall match SKI of issuing CA Certificate

CRL Entry Extension	Required	Critical	Value
Reason Code	Optional	False	Shall be included when reason code is equal to *key compromise* or *CA compromise*
Invalidity Date	Optional	False	

OCSP Response Profile

OCSP Responders under this profile are expected to operate using the Static Response model described in RFC 6960 and thus will not support nonce.

Field	Value and Requirements
Response Status	As specified in RFC 6960
Response Type	id-pkix-ocsp-basic {1.3.6.1.5.5.7.48.1.1}
Version	V1 (0x0)
Responder ID	By Key Identical to subject key identifier in Responder Certificate
Produced At	The time at which the response was encoded and signed
Responses	Sequence of one or more Single Response as specified below
Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Most recent certificate issued to the OCSP Responder by the CA identified by the issuerNameHash and issuerKeyHash in the Single Responses included in the response

Extension	Required	Critical	Value and Requirements
Nonce	Not Supported	N/A	Nonce is not supported

Single Response

Field	Value and Requirements
CertID	hashAlgorithm SHALL be SHA1 The issuerKeyHash and issuerNameHash pair must be identical within all Single Responses appearing in an OCSP Response
Certificate Status	Determined by CRL If revoked, revocationReason is included if present on the CRL
This Update	Identical to the thisUpdate of the CRL used for determining revocation status
Next Update	Before or identical to the nextUpdate field of the CRL used for determining revocation status
Single Extensions	Optional: Transparency Information X.509v3 Extension {1 3 101 75}